IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Confirmation No.: 3018
BELANGER *et al.*	Art Unit: 2436
Appl. No.: 10/659,368	Examiner: Johnson, Carlton
Filed: September 11, 2003	Atty. Docket: 2222.3810000
For: **System and Method for Data Access and Control**	

Brief on Appeal Under 37 C.F.R. § 41.37

Mail Stop Appeal Brief - Patents

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

A Notice of Appeal from the final Office Action, dated January 7, 2011, was filed on April 6, 2011. Appellants hereby files one copy of this Appeal Brief, together with the required fee set forth in 37 C.F.R. § 41.20(b)(2).

It is not believed that extensions of time are required beyond those that may otherwise be provided for in documents accompanying this paper. However, if additional extensions of time are necessary to prevent abandonment of this application, then such extensions of time are hereby petitioned under 37 C.F.R. § 1.136(a), and any fees required therefor (including fees for net addition of claims) are hereby authorized to be charged to our Deposit Account No. 19-0036.

Table of Contents

I. Real Party in Interest (37 C.F.R. § 41.37(c)(1)(i))

The real party in interest in this appeal is Voice Signals L.L.C., having its principal place of business at 2215-B Renaissance Drive, Suite 5, Las Vegas, Nevada 89119. An Assignment assigning all right, title, and interest in and to the patent application from the inventors to General Dynamics Decision Systems, Inc. was recorded in the Assignment Branch of the United States Patent and Trademark Office on February 5, 2004, at reel 014954, frame 0691.

An Assignment assigning all right, title, and interest in and to the patent application from General Dynamics Decision Systems, Inc. to General Dynamics C4 systems, Inc. was recorded in the Assignment Branch of the United States Patent and Trademark Office on March 22, 2006, at reel 017347, frame 0314.

An Assignment assigning all right, title, and interest in and to the patent application from General Dynamics C4 systems, Inc. to Voice Signals L.L.C. was recorded in the Assignment Branch of the United States Patent and Trademark Office on February 10, 2006, at reel 017154, frame 0330.

II. Related Appeals and Interferences (37 C.F.R. § 41.37(c)(1)(ii))

To the best of the knowledge of Appellants, Appellants' legal representative, and Appellants' assignee, there are no other appeals, interferences, or judicial proceedings which are related to, directly affect, or be directly affected by or have a bearing on a decision by the Board of Patent Appeals and Interferences ("the Board") in the pending appeal.

III. Status of Claims (37 C.F.R. § 41.37(c)(1)(iii))

Claims 1-37 were originally filed on September 11, 2003. A non-final Office Action was mailed January 22, 2007 ("First Non Final Office Action"), in which claims 1-37 were rejected. An Amendment and Reply under 37 C.F.R. § 1.111 was filed July 23, 2007, in which amendments to claims 1-3, 7-9, 15-18, 23-25, and 29-32 were requested ("First Reply"). A final Office Action was mailed October 4, 2007 ("First Final Office Action"), in which claims 1-37 were finally rejected. An Amendment and Reply under 37 C.F.R. § 1.116 was filed November 19, 2007 ("Second Reply"), in which amendments to claims 24, 29, and 30 were requested. An Advisory Action was mailed December 13, 2007 ("First Advisory Action"). The Examiner maintained the rejections set forth in the First Final Office Action and the claim amendments requested were entered for purposes of appeal.

A Request for Continued Examination (RCE), together with a Preliminary Amendment under 37 C.F.R. § 1.115 was filed on January 4, 2008, in which claim 30 was sought to be amended and new claims 38-40 were sought to be added ("Third Reply"). A non-final Office Action was mailed April 2, 2008 ("Second Non Final Office Action"), in which claims 1-40 were rejected. An Amendment and Reply under 37 C.F.R. § 1.111 was filed July 2, 2008, in which claims 1, 4-8, 10-16, 19-24, 26-31, and 33-40 were sought to be amended ("Fourth Reply"). A telephone interview was held with the Examiner on July 16, 2008. A final Office Action was mailed October 22, 2008 ("Second Final Office Action"), in which claims 1-40 were finally rejected. An Amendment and Reply under 37 C.F.R. § 1.116 was filed December 22, 2008 ("Fifth Reply"), in which claim 15 was sought to be amend for clarity. An Advisory Action was mailed January 13, 2009 ("Second Advisory Action"). The Examiner maintained the rejections set forth in the Second Final Office Action and the claim amendments requested were entered for purposes of appeal. A Notice of Appeal and a Pre

Appeal Conference Argument were filed March 23, 2009 ("Argument"). A Panel Decision reopening the prosecution and withdrawing the rejection, and passing this application to the Examiner, was mailed April 13, 2009 ("Panel Decision").

A non-final Office Action was mailed June 24, 2009 ("Third Non Final Office Action"), in which claims 1-40 were rejected. A telephone interview was held with the Examiner on September 17, 2009. An Amendment and Reply under 37 C.F.R. § 1.111 was filed September 24, 2009, in which claims 7, 23, 24, 29, and 30 were sought to be amended and claims 41 and 42 were sought to be added ("Sixth Reply"). A final Office Action was mailed January 4, 2010 ("Third Final Office Action"), in which claims 1-42 were finally rejected. An Amendment and Reply under 37 C.F.R. § 1.116 was filed March 3, 2010 ("Seventh Reply"), in which no claim was sought to be amended. An Advisory Action was mailed March 23, 2010 ("Third Advisory Action"). The Examiner maintained the rejections set forth in the Third Final Office Action.

A Request for Continued Examination (RCE), together with a Preliminary Amendment under 37 C.F.R. § 1.115 was filed on May 26, 2010, in which claims 1-38 and 41 were sought to be amended, claims 39 and 40 were sought to be cancelled, and claims 43 and 44 were sought to be added ("Eight Reply"). A non-final Office Action was mailed July 19, 2010 ("Fourth Non Final Office Action"), in which claims 1-38 and 41-44 were rejected. An Amendment and Reply under 37 C.F.R. § 1.111 was filed October 18, 2010, in which claims 1-5, 7-11, 13, 15-18, 20, 24, 29, 30, and 32 were sought to be amended ("Ninth Reply"). A final Office Action was mailed January 7, 2011 ("Fourth Final Office Action"), in which claims 1-38 and 41-44 were finally rejected. An Amendment and Reply under 37 C.F.R. § 1.116 was filed March 7, 2011 ("Ninth Reply"), in which claims 1, 15, 24, and 28 were sought to be amended. An Advisory Action was mailed March 24, 2011 ("Fourth

Advisory Action"). The Examiner maintained the rejections set forth in the Fourth Final Office Action and the claim amendments requested were entered for purposes of appeal.

Claims 1-38 and 41-44 are pending. Claims 39 and 40 were previously cancelled. Claims 1-38 and 41-44 are finally rejected and are being appealed. A copy of the claims on appeal are set forth in the attached Claims Appendix as required under 37 C.F.R. § 41.37(c)(1)(viii).

IV. Status of Amendments (37 C.F.R. § 41.37(c)(1)(iv))

No amendments have been filed subsequent to the Fourth Final Advisory Action dated March 24, 2011. All amendments to the claims previously presented during prosecution have been entered.

V. Summary of Recited Subject Matter (37 C.F.R. § 41.37(c)(1)(v))

A concise explanation of the subject matter recited in each of the independent claims on appeal (i.e., claims 1, 7, 15, 16, 23, 24, 29, and 30) is provided below. The explanation refers to the specification by page and line number and to the drawings by reference characters. Reference is made to example supporting embodiments disclosed in the specification, although it is understood that the claims should not be limited to the specific embodiments to which reference is made.

Each independent claim involved in the appeal, and every means plus function and step plus function as permitted by 35 U.S.C. § 112, sixth paragraph, are identified. Example structure, material, or acts described in the specification as corresponding to each recited function are set forth with reference to the specification by page and line number or paragraph number, and to the drawings, if any, by reference characters.

A. Independent Claim 1

Claim 1 recites a method that comprises:

- receiving, using a processing device, a first request, from a first sponsor of an access candidate, for access to a first security level in a computer network, wherein the first security level secures computational resources for accessing electronic data (e.g., Pg. 6, Lns. 24-25; Pg. 8, Lns. 19-27);

- determining, using the processing device, whether access candidate attributes satisfy access requirements of the resources (e.g., Pg. 6, Lns. 25-26; Pg. 9, Lns. 1-20), wherein the access candidate attributes are revisable based, at least in part, on a determination indicating that access to the first level is prohibited (e.g., Pg. 9, Lns. 23-30; Pg. 11, Ln. 29 - Pg. 12, Ln. 2);

- granting, using the processing device, access to the first security level based on a determination indicating that access to the first level is not prohibited (e.g., Pg. 6, Lns. 27-28; Pg. 10, Lns. 1-6);

- receiving, using the processing device, a second request, from a second sponsor of the access candidate, for access to a second security level in the computer network in response to the granting of access to the first security level, wherein the second security level secures the electronic data (e.g., Pg. 6, Lns. 27-28; Pg. 10, Lns. 10-11 and Lns. 24-30);

- determining, using the processing device, whether the access candidate attributes satisfy access requirements of the electronic data (e.g., Pg. 6, Ln. 28 - Pg. 7, Ln 3; Pg. 11, Lns. 1-5 and Lns. 15-19);

- obtaining authorization for the second request from a resolution authority if the access candidate attributes fail to satisfy the access requirements of the electronic data in response to a determination indicating that access to the second security level is prohibited (e.g., Pg. 7, Lns. 2-5; Pg. 11, Lns. 20-28); and

- in response to obtaining the authorization from the resolution authority, granting access to the second security level (e.g., Pg. 11, Lns. 25-28; Pg. 16, Lns.4-14).

B. Independent Claim 7

Claim 7 recites a method that comprises:

- receiving, using a processing device, a first request, from a first sponsor of an access candidate, for physical access to a computer network (e.g., Pg. 6, Lns. 24-25; Pg. 8, Lns. 19-27);

- determining, using the processing device, whether access candidate attributes satisfy access requirements of physical access, (e.g., Pg. 6, Lns. 25-26; Pg. 9, Lns. 1-20), wherein the access candidate attributes are revisable based, at least in part, on a determination indicating that physical access is prohibited (e.g., Pg. 9, Lns. 23-30; Pg. 11, Ln. 29 - Pg. 12, Ln. 2);

- granting, using the processing device, the physical access to the computer network based on a determination indicating that physical access is not prohibited (e.g., Pg. 6, Lns. 27-28; Pg. 10, Lns. 1-6);

- receiving, using the processing device, a second request, from a second sponsor of the access candidate, for access to electronic data in the computer network in response to the granting of physical access to the computer network (e.g., Pg. 6, Lns. 27-28; Pg. 10, Lns. 10-11 and Lns. 24-30);

- determining, using the processing device, whether the access candidate attributes satisfy access requirements of the electronic data (e.g., Pg. 6, Ln. 28 - Pg. 7, Ln 3; Pg. 11, Lns. 1-5 and Lns. 15-19);

- obtaining authorization for the second request from a resolution authority if the access candidate attributes fail to satisfy access requirements of the electronic data in response to a determination indicating that access to the electronic data is prohibited (e.g., Pg. 7, Lns. 2-5; Pg. 11, Lns. 20-28); and

- in response to obtaining the authorization from the resolution authority, granting access to the electronic data (e.g., Pg. 11, Lns. 25-28; Pg. 16, Lns.4-14).

C. Independent Claim 15

Claim 15 recites a method that comprises:

- identifying, using a processing device, a plurality of data subsets of electronic data, wherein respective data subsets correspond to respective sets of access requirements (e.g., Pg. 12, Lns. 12-21);

- determining, using the processing device, at least one data class associated with the respective data subsets, the at least one data class identifying at least a citizenship requirement and a location requirement for access to data associated with the at least one data class (e.g., Pg. 12, Lns. 21-27; Pg. 17, Ln. 30 - Pg. 18, Ln 6);

- receiving, using the processing device, a first request, from a first sponsor of an access candidate, for access to a first security level in a computer network, wherein the first security level secures physical access to a computer workstation for accessing the electronic data, the first request including access attributes of the access candidate (e.g., Pg. 6, Lns. 24-25; Pg. 8, Lns. 19-27) comprising an indication of a citizenship status of the access candidate, an indication of a current location of the access candidate, and an indication of an existence of a data access agreement with the access candidate (e.g., Pg. 9, Lns. 5-12; Pg. 16, Lns. 24-26);

- determining, using the processing device, whether the access candidate attributes satisfy access requirements of the first security level, wherein the access candidate attributes are revisable based, at least in part, on a

determination indicating that access to the first security level is prohibited (e.g., Pg. 9, Lns. 23-30; Pg. 11, Ln. 29 - Pg. 12, Ln. 2);

- granting, using the processing device, access to the first security level based on a determination indicating that access to the first security level is not prohibited (e.g., Pg. 6, Lns. 27-28; Pg. 10, Lns. 1-6);

- receiving, using the processing device, a second request, from a second sponsor of the access candidate, for access to a second security level in the computer network in response to the granting of access to the first security level, wherein the second security level secures access to at least one of the plurality of data subsets (e.g., Pg. 6, Lns. 27-28; Pg. 10, Lns. 10-11 and Lns. 24-30);

- determining, using the processing device, whether the access candidate attributes satisfy the respective set of access requirements corresponding to the at least one of the plurality of data subsets (e.g., Pg. 6, Ln. 28 - Pg. 7, Ln 3; Pg. 11, Lns. 1-5 and Lns. 15-19);

- obtaining authorization for the second request from a resolution authority if the access candidate attributes fail to satisfy the respective set of access requirements corresponding to the at least one of the plurality of data subsets in response to a determination indicating that access to the at least one of the plurality of data subsets is prohibited (e.g., Pg. 7, Lns. 2-5; Pg. 11, Lns. 20-28); and

- in response to obtaining the authorization from the resolution authority, granting access to the second security level (e.g., Pg. 11, Lns. 25-28; Pg. 16, Lns.4-14).

D. Independent Claim 16

Claim 16 recites a system that comprises:

- storage means for receiving and storing (e.g., Pg. 7, Lns. 14-16; FIG.1, elements 134, 138, 140, 142) electronic data using a computer network (e.g., Pg. 7, Lns. 11-13 and Lns. 14-16);

- means for evaluating (e.g., Pg. 7, Ln. 29 - Pg. 8, Ln 9; FIG.1, element 104; FIG. 2, element 208) a first request for access to one or more resources in the computer network, wherein the resources secure the electronic data, wherein an evaluation of the first request includes a first comparison of one or more attributes of the access candidate with one or more access requirements associated with the resources (e.g., Pg. 6, Lns. 24-25; Pg. 8, Ln. 19 - Pg. 9, Ln. 20), and wherein the one or more attributes of the access candidate are revisable if the first comparison indicates that access is prohibited (e.g., Pg. 9, Lns. 23-30; Pg. 11, Ln. 29 - Pg. 12, Ln. 2);

- means for granting access (e.g., Pg. 10, Lns. 1-3; FIG. 1, element 104; FIG. 2, element 208) to the one or more resources if the first comparison indicates that access is not prohibited (e.g., Pg. 6, Lns. 27-28; Pg. 10, Lns. 1-6);

- means for evaluating (e.g., Pg. 10, Lns. 10-11; FIG. 1, element 106; FIG. 3, elements 306 and 308) a second request for access to the electronic data by the one or more resources, wherein an evaluation of the second request includes a

second comparison of the one or more attributes of the access candidate with one or more access requirements associated with the electronic data (e.g., Pg. 6, Ln. 27 - Pg. 7, Ln 3; Pg. 10, Lns. 10-11 and Lns. 24-30; Pg. 11, Lns. 1-5 and Lns. 15-19);

- means for obtaining authorization (e.g., Pg. 11, Lns. 20-22; FIG. 1, element 106; FIG. 3, elements 306 and 308) for the second request form a resolution authority (e.g., Pg. 11, Lns. 20-22; FIG. 1, element 124; FIG. 3, element 320) if the one or more attributes of the access candidate fails to satisfy one or more access requirements associated with the electronic data in response to the evaluation of the second request indicating that access to the electronic data is prohibited (e.g., Pg. 7, Lns. 2-5; Pg. 11, Lns. 20-28; Pg. 15, Lns. 24-30); and

- means for granting (e.g., Pg. 11, Lns. 25-28; element 106; FIG. 3, elements 306 and 308), in response to obtaining the authorization from the resolution authority, the access candidate access to the electronic data using the one or more resources (e.g., Pg. 11, Lns. 25-28; Pg. 16, Lns.4-14).

E. Independent Claim 23

Claim 23 recites a system that comprises:

- storage (e.g., Pg. 7, Lns. 14-16; FIG.1, elements 134, 138, 140, 142) configured to receive and store electronic data using a computer network (e.g., Pg. 7, Lns. 11-13 and Lns. 14-16);

- one or more resources configured to process and manipulate the electronic data using a computer network (e.g., Pg. 6, Lns. 21-25; Pg. 8, Lns. 3-9; FIG.1, element 110);

- a resource access controller (e.g., Pg. 7, Ln. 29 - Pg. 8, Ln 9; FIG.1, element 104; FIG. 2, element 208) configured to grant access to one or more resources, in response to a request for access to the one or more resources (e.g., Pg. 6, Lns. 24-25; Pg. 8, Ln. 19 - Pg. 9, Ln. 20), based at least in part on a comparison of a citizenship status and a current location of an access candidate and an existence of a data access agreement with a citizenship requirement, wherein the location requirement and the data access agreement requirement are associated with the one or more resources (e.g., Pg. 6, Lns. 27-28; Pg. 9, Lns. 5-12; Pg. 10, Lns. 1-6; Pg. 16, Lns. 24-26);

- one or more data access controllers (e.g., Pg. 10, Lns. 10-11; FIG. 1, element 106; FIG. 3, elements 306 and 308) configured to grant access to a corresponding portion of the electronic data based at least in part on a comparison of the citizenship status and the current location of the access candidate with the citizenship requirement and the location requirement associated with the one or more data classes of the corresponding portion of the electronic data (e.g., Pg. 6, Ln. 27 - Pg. 7, Ln 3; Pg. 10, Lns. 10-11 and Lns. 24-30; Pg. 11, Lns. 1-5 and Lns. 15-19);

- one or more resolution authorities to (e.g., Pg. 11, Lns. 20-22; FIG. 1, element 124; FIG. 3, element 320) configured to:

  - modify access requirements associated with the one or more data classes (e.g., Pg. 11, Lns. 25-28), and

  - authorize access to one or more portions of the electronic data in response to a comparison performed by a corresponding data access controller indicating

that access is prohibited (e.g., Pg. 11, Ln. 20 - Pg. 12, Ln. 2; Pg. 15, Ln. 24 - Pg. 16, Ln. 9); and

- a data access module (e.g., Pg. 12, Lns. 12-27; FIG. 1, element 106; FIG. 3, elements 306 and 308) configured to:

- evaluate a request for access to one or more portions of the electronic data using the one or more resources (e.g., Pg. 12, Lns. 21-27),

- identify one or more data access controllers corresponding to the one or more portions of the electronic data (e.g., Pg. 12, Lns. 12-21), and

- forward the request for access to the one or more identified data access controllers for evaluation regarding whether to grant access to the corresponding one or more portions of the electronic data (e.g., Pg. 15, Ln. 24 - Pg. 16, Ln. 14).

F. Independent Claim 24

Claim 24 recites a method that comprises:

- receiving, using a controller in a computer network associated with secured electronic data, a request for access to secured electronic data in the computer network (e.g., Pg. 6, Lns. 27-28; Pg. 10, Lns. 10-11 and Lns. 24-30);

- comparing, using the controller, one or more attributes of an access candidate with one or more access requirements associated with the secured electronic data (e.g., Pg. 6, Ln. 28 - Pg. 7, Ln 3; Pg. 11, Lns. 1-5 and Lns. 15-19);

- obtaining authorization for the request from a resolution authority if one or more attributes of the access candidate fails to satisfy one or more access requirements associated with the secured electronic data (e.g., Pg. 7, Lns. 2-5; Pg. 11, Ln. 20-28; Pg. 15, Lns. 24-30); and

- in response to obtaining or not obtaining authorization from the resolution authority, granting or denying in whole or in part, using the controller, access to the secured electronic data based, at least in part, on a determination based on access candidate information and request related information (e.g., Pg. 11, Ln. 25 - Pg. 12, Ln. 11; Pg. 16, Lns.4-14),

- wherein the one or more attributes of the access candidate are revisable based, at least in part, on a determination denying access to the secured electronic data (e.g., Pg. 9, Lns. 23-30; Pg. 11, Ln. 29 - Pg. 12, Ln. 2).

G. Independent Claim 29

Claim 29 recites a method that comprises:

- receiving, using a controller in a computer network associated with secured electronic data in the computer network, a request for access to the secured electronic data in the computer network (e.g., Pg. 6, Lns. 27-28; Pg. 10, Lns. 10-11 and Lns. 24-30);

- comparing, using the controller, one or more attributes of an access candidate with one or more access requirements associated with the secured electronic data (e.g., Pg. 6, Ln. 28 - Pg. 7, Ln 3; Pg. 11, Lns. 1-5 and Lns. 15-19);

- granting, using the controller, access to the secured electronic data in response to a comparison indicating that access by the access candidate is not prohibited (e.g., Pg. 7, Ln. 28 - Pg. 7, Ln. 1; Pg. 10, Lns 24-30; Pg. 12, Ln. 3-11);

- obtaining authorization for the request from a resolution authority in response to a comparison indicating that access by the access candidate is prohibited (e.g., Pg. 7, Lns. 2-5; Pg. 11, Ln. 20-28; Pg. 15, Lns. 24-30);

- in response to obtaining or not obtaining authorization from the resolution authority, granting or denying in whole or in part, using the controller access to the secured electronic data based, at least in part, on a determination based on access candidate information and request related information (e.g., Pg. 11, Ln. 25 - Pg. 12, Ln. 11; Pg. 16, Lns.4-14),

- wherein the one or more attributes of the access candidate are revisable based, at least in part, on a determination denying access to the secured electronic data (e.g., Pg. 9, Lns. 23-30; Pg. 11, Ln. 29 - Pg. 12, Ln. 2).

H. Independent Claim 30

Claim 30 recites an article of manufacture including a non-transitory computer-readable medium (e.g., Para. [0050] as amended in the Amendment and Reply filed on October 18, 2010) having instructions stored thereon, execution of which causes a processing device to perform operations comprising:

- receiving, using a processing device, a request for access to a first security level in a computer network (e.g., Pg. 6, Lns. 24-25; Pg. 8, Lns. 19-27);

- comparing, using the processing device, one or more attributes of an access candidate with one or more access requirements associated with the first security level, (e.g., Pg. 6, Lns. 25-26; Pg. 9, Lns. 1-20), wherein the one or more attributes of the access candidate are revisable based, at least in part, on a determination indicating that access by the access candidate to the first security level is prohibited (e.g., Pg. 9, Lns. 23-30; Pg. 11, Ln. 29 - Pg. 12, Ln. 2);

- granting, using the processing device, access to the first security level based on a comparison indicating that access by the access candidate to the first security level is not prohibited (e.g., Pg. 6, Lns. 27-28; Pg. 10, Lns. 1-6);

- receiving, using the processing device, a request for access to a second security level in the computer network (e.g., Pg. 6, Lns. 27-28; Pg. 10, Lns. 10-11 and Lns. 24-30);

- obtaining authorization for the request from a resolution authority in response to a comparison indicating that access by the access candidate is prohibited (e.g., Pg. 7, Lns. 2-5; Pg. 11, Lns. 20-28).

Each of independent claims 1, 7, 15, 16, 23, 24, 29, and 30 finds support ***at least*** in the above-referenced sections of the Specification. The remaining claims draw support from the aforementioned sections of the Specification.

VI. Grounds of Rejection To Be Reviewed on Appeal (37 C.F.R. § 41.37(c)(1)(vi))

In the Final Office Action dated January 7, 2011, the Examiner alleged the following rejections.

Claims 1-4, 7-10, 14, 16-19, 24-26, 29-33, 37, and 38 were rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over U.S. Patent No. 6,041,412 to Timson *et al.* ("Timpson") in view of U.S. Patent No. 6,959,336 to Moreh *et al.* ("Moreh") and further in view of U.S. Patent No. 6,839,843 to Bacha *et al.* ("Bacha").

Claims 5, 6, 11-13, 15, 20-23, 27, 28, 34-36, and 41-44 were rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Timson in view of Moreh, further in view of Bacha, and still further in view of U.S. Patent Application Publication No. 2004/0049687 to Orsini *et al.* ("Orsini").

VII. Argument (37 C.F.R. § 41.37(c)(1)(vii))

There are two grounds of rejection to be reviewed on appeal.

A. Claims 1-4, 7-10, 14, 16-19, 24-26, 29-33, 37, and 38 are not rendered obvious by the combination of Timson, Moreh, and Bacha

The Examiner rejected claims 1-4, 7-10, 14, 16-19, 24-26, 29-33, 37, and 38 under 35 U.S.C. § 103(a) in the Final Office Action dated January 7, 2011, as allegedly being unpatentable over Timson in view of Moreh and further in view of Bacha.

Claims 1, 7, 16, 24, 29, and 30 are the independent claims. Independent claim 1 recites at least the following distinguishing feature: "wherein ***the access candidate attributes are revisable based, at least in part, on a determination indicating that access to the first level is prohibited.***" Independent claims 7, 16, 24, 29, and 30 recite similar distinguishing features, using analogous language.

Timson, Moreh, and Bacha, taken alone or in combination do not teach or suggest at least the above-noted distinguishing features, and the Examiner's continued rejection based on 35 U.S.C. § 103(a) is therefore clearly erroneous as being legally and factually deficient.

1. Timson and Moreh cannot be combined

Appellants maintain that the teachings of Timson and Moreh cannot be combined.

The Examiner, on pages 7 and 8 of the Final Office Action of January 7, 2011 (Fourth Final Office Action) states (*emphasis added*):

> Furthermore, ***Timson discloses access determination using additional authorization modules***. (see Timson col. 4, line 60 – col. 5, line 4: additional authorization modules) ...
>
> Timson does not specifically disclose a resolution authority or a 3rd party providing authentication services. ...
>
> ***It would have been obvious to one of ordinary skill in the art to modify Timson to use authentication services such as a resolution authority as taught by Moreh. One of ordinary skill in the art would have*** been motivated to employ the teachings of Moreh in order to permit users and service provides [sic] the flexibility of choosing where to authenticate. (see Moreh col. 2, lines 44-46).

Appellants respectfully disagree. It would not make sense to modify Timson to use authentication services taught by Moreh. As discussed in more detail below, Timson merely teaches a dual secure data module scheme. Contrary to the Examiner's suggestion, there is no teaching or suggestion in Timson that additional layers of authentication services can be added to this dual scheme.

The Timson arrangement includes a dual secure data module scheme: an interrogatable module (IM) and an enable module (EM). In the case that EM does not have appropriate permissions, no data communication is allowed and also if the EM does not provide the necessary permissions, the IM prevents the EM to access the requested data (Timson col. 3, line 11 to col. 4, line 15, and also col. 13, line 22 to col. 14, line 40).

Moreh teaches "a federated authentication service technology ... for authenticating a subject ... residing in a subject domain ... on a network to a server application ... residing in a server domain" (Moreh, Abstract).

The Examiner suggests that it would be apparent to one of ordinary skill to modify Timson to add another layer of authentication (for example, the authentication service of Moreh) thereby meeting the limitation "resolution authority" of the independent claims. The Examiner, on page 7 of the Final Office Action of January 7, 2011 (Fourth Final Office Action) states (*emphasis added*):

> Furthermore, ***Timson discloses access determination using additional authorization modules***. (see Timson col. 4, line 60 – col. 5, line 4: additional authorization modules)

Appellants respectfully disagree. Timson teaches that "using the structure shown in FIGS. 1-5, a completely hierarchical secure data system can be created and implemented in the form of a dual secure data module scheme including a security scheme which only allows data operations and communications between secure data modules belonging to a common security scheme" (Timson, column 11, line 65 - column 12, line 4). However, the hierarchical data system of Timson is nevertheless implemented in the form of ***dual secure data module scheme*** (as explained in more detail below). There is no teaching or suggestion in Timson that the authentication process (or access determination) can use additional authorization modules as the Examiner suggests. The authentication process of Timson only involves one EM and one IM that communicate with each other to provide access to secured data and no additional security level could be added to this authentication process and if EM does not have the necessary permissions, access to the secured data is denied. There is no way to add to Timson an additional authorization module, such as taught by Moreh.

The dual secure data module scheme of Timson is explained in more detail here. Timson provides access to secured data or area that includes at least two secure data modules, an interrogatable module (IM) and an enable module (EM). In Timson's system, it is "determine[d] whether the enabling module is authorized to perform data operations on data

contained on the interrogatable module" (Thomson column 3, lines 14-16). "[I]n response to the challenge from the interrogatable module ... the enabling module issues a response ... informing that ... whether the enabling module has permission to perform data operations on the interrogatable module data" (Thomson column 3, lines 21-27). "If it is determined that the enabling module does not have the appropriate permissions ... the response from the enabling module is negative and no data communication is allowed" (Thomson column 3, lines 28-33). Further, "[t]he interrogatable module will respond to the request [for data] from the enabling module by issuing a challenge to the enabling module ... to determine whether the permissions stored on the enabling module allow the enabling module to access the requested data stored on the interrogatable module. If the enabling module does not provide the necessary permissions data in form of a response to the challenge, ... the interrogatable module prevent[s] the requested data from being accessed by the enabling module" (Thomson column 4, lines 1-15). Therefore, if the IM determines that the EM does not have appropriate permissions for data operation (and/or necessary permission for data access), the data communication (and/or the access to secured data) is denied.

Since there is no way in authentication process of Timson to add an <u>additional</u> authorization module, such as taught by Moreh, thus, Appellants maintain that Timson and Moreh cannot be combined to establish a prima facie case of obviousness, and therefore the rejection of claims 1, 7, 16, 24, 29, and 30 is in error and cannot be sustained. Accordingly, on this basis alone, Appellants respectfully request withdrawal of the erroneous rejection of claims 1, 7, 16, 24, 29, and 30.

2. Claims 1, 7, 16, 24, 29, and 30: The combination of Timson, Moreh, and Bacha does not teach or suggest "wherein the access candidate attributes are revisable based, at least in part, on a determination indicating that access to the first level is prohibited"

Assuming, *arguendo,* that Timson and Moreh can be combined, which Appellants do not agree, Timson and Moreh, taken alone or in combination, do not teach or suggest "wherein the access candidate attributes are revisable based, at least in part, on a determination indicating that access to the first level is prohibited" of independent claims 1, 7, 16, 24, 29, and 30, using their respective language (as admitted by the Examiner at least at page 8 of Fourth Final Office Action).

The Examiner states that the claim feature "wherein the access candidate attributes are revisable based, at least in part, on a determination indicating that access to the first level is prohibited" is disclosed in column 16, lines 48-60 of Bacha (Fourth Final Office Action, pages 3 and 8 and Fourth Advisory Action, page 2). Appellants respectfully disagree. Bacha teaches "the ability to update the given ***document's access control***" (Bacha, column 10, lines 48-50), while the claims recite ***access candidate attributes*** are revisable.

The "access control" disclosed in Bacha is associated with a given "document". In contrast, the "access candidate attributes" of independent claims are associated with the "access candidate". Therefore, the "access candidate attributes" of the claims are <u>not</u> the same as the "document's access control" of Bacha.

Further, the Examiner has been inconsistent in applying the "***document's access control***" of Bacha to features of the independent claims. For example, claim 1 recites "access candidate attributes" that are associated with the access candidate and "access requirements of the resources" (or "access requirements of the electronic data") that are associated with the resources (or the electronic data). The Examiner, in the Non-Final Office Action of July 19,

2010 (Fourth Non Final Office Action), used the same section of Bacha to allegedly reject the "the resolution authority *modifies the access requirements*" feature, which was previously presented in the claims. Thus, the Examiner previously analogized the "access requirements" associated to the resources or the electronic data of independent claims to the "document's access control" of Bacha. However, in the Fourth Final Office Action, the Examiner is using "document's access control" of Bacha to allegedly show "access candidate attributes". Appellants respectfully disagree.

The "access candidates attributes" of independent claims 1, 7, 16, 24, 29, and 30 are associated with the access candidate. In contrast, the "document's access control" of Bacha is associated with the document. Bacha's modification to the access list of a document is not the same or similar to access candidate attributes being revisable based, at least in part, on a determination that an access is denied, as recited in independent claims 1, 7, 16, 24, 29, and 30, using their respective language.

Thus, as Bacha fails to cure the deficiencies of Timson and Moreh as noted above, the applied references cannot be used to establish a prima facie case of obviousness, and therefore the rejection of claims 1, 7, 16, 24, 29, and 30 is in error and cannot be sustained. Accordingly, on this basis alone, Appellants respectfully request withdrawal of the erroneous rejection of claims 1, 7, 16, 24, 29, and 30.

At least based on their respective dependencies to claims 1, 7, 16, 24, and 30, claims 2-4, 8-10, 14, 17-19, 25, 26, 31-33, 37, and 38 should be found allowable over the applied references, as well as for their respective additional distinguishing features.

B. Claims 5, 6, 11-13, 15, 20-23, 27, 28, 34-36, and 41-44 are not rendered obvious by the combination of Timson, Moreh, Bacha, and Orsini

The Examiner rejected claims 5, 6, 11-13, 15, 20-23, 27, 28, 34-36, and 41-44 under 35 U.S.C. § 103(a) in the Final Office Action dated January 7, 2011, as allegedly being unpatentable over Timson in view of Moreh, further in view of Bacha, and in further view of Orsini.

Claims 15 and 23 are the independent claims. Independent claim 15 recites at least the following distinguishing feature: "determining, using the processing device, whether the access candidate attributes satisfy access requirements of the first security level, ***wherein the access candidate attributes are revisable based, at least in part, on a determination indicating that access to the first security level is prohibited.***" Independent claim 23 recites at least the following distinguishing feature: "***identify one or more data access controllers corresponding to the one or more portions of the electronic data***" and "***forward the request for access to the one or more identified data access controllers for evaluation*** regarding whether to grant access to the corresponding one or more portions of the electronic data."

Timson, Moreh, Bacha, and Orsini taken alone or in combination do not teach or suggest at least the above-noted distinguishing features, and the Examiner's continued rejection based on 35 U.S.C. § 103(a) is therefore clearly erroneous as being legally and factually deficient.

1. Claim 15: The combination of Timson, Moreh, Bacha, and Orsini does not teach or suggest "wherein the access candidate attributes are revisable based, at least in part, on a determination indicating that access to the first security level is prohibited"

As discussed above, Timson, Moreh, and Bacha taken alone or in combination do not disclose or suggest the above-noted distinguishing features of claim 15.

Further, on pages 19-20 of the Fourth Final Office Action the Examiner states that Orsini allegedly teaches, which Appellants do not acquiesce to, "b) at least a citizenship requirement and a location requirement for access to data associated with the at least one data class;" and "c) an indication of a citizenship status of the access candidate, an indication of a current location of the access candidate, and an indication of an existence of a data access agreement with the access candidate". However, Orsini is not cited as disclosing, nor does it disclose at least the above-noted distinguishing features of claim 15. Thus, Orsini does not cure the deficiencies of Timson, Moreh, and Bacha as noted above. These applied references do not establish a prima facie case of obviousness. Accordingly, Appellants respectfully request reconsideration and withdrawal of the erroneous rejection of independent claim 15.

2. Claim 23: The combination of Timson, Moreh, Bacha, and Orsini does not teach or suggest "identify one or more data access controllers corresponding to the one or more portions of the electronic data" and "forward the request for access to the one or more identified data access controllers for evaluation regarding whether to grant access to the corresponding one or more portions of the electronic data."

The Examiner, at pages 4, 23, and 24 of the Fourth Final Office Action, relies on Timson to allegedly show "identify one or more data access controllers corresponding to the one or more portions of the electronic data" and "forward the request for access to the one or more identified data access controllers for evaluation regarding whether to grant access to the corresponding one or more portions of the electronic data," of independent claim 23. Appellants respectfully disagree.

The Examiner, in response to Appellants' arguments and at page 4 of the Fourth Final Office Action, relies on column 3, lines 34-40 and 57-64 and column 2, lines 31-34 and 40-41 of Timson, to allegedly teach, which Appellants do not acquiesce to, "forward the request for access to the one or more identified data access controllers for evaluation," as recited in claim 23. However, the Examiner does not state how Timson allegedly teaches "identify one or more data access controllers corresponding to the one or more portions of the electronic data," as recited in claim 23.

As discussed above, Timson discloses an interrogatable module (IM) and an enable module (EM) that communicate with each other to evaluate permissions for data access and/or operations (Thomson column 3, lines 14 - column 4, line 15). However, there is no teaching or suggestion that Timson's system is able to identify one or more data access controllers and to forward a request to the identified data access controllers for evaluation of granting access, as disclosed in claim 23, using its respective language.

Further, Moreh, Bacha, and Orsini are not used to disclose, nor do Moreh, Bacha, and Orsini teach or suggest, at least the above-noted distinguishing features of claim 23. Thus, as Moreh, Bacha, and Orsini fail to cure the deficiencies of Timson as noted above, the applied references cannot be used to establish a prima facie case of obviousness. Therefore the rejection of claim 23 is in error and cannot be sustained. Accordingly, Appellants respectfully request reconsideration and withdrawal of the erroneous rejection of independent claim 23.

Also, at least based on their respective dependencies to claims 1, 7, 15, 16, 24, and 30, claims 5, 6, 11-13, 20-22, 27, 28, 34-36, and 41-44 should be found allowable over the applied references, as well as for their respective additional distinguishing features.

C. Conclusion

The applied references do not support rejections of claims 1-38 and 41-44 because the Examiner has failed to establish obviousness of at least the above distinguishing features. Therefore, Appellants respectfully request that the Board reverse the Examiner's final rejection of these claims under 35 U.S.C. § 103(a), and remand this application for allowance of claims 1-38 and 41-44.

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.

Glenn J. Perry
Attorney for Applicants
Registration No. 28,458

Date: 6 June 2011

1100 New York Avenue, N.W.
Washington, D.C. 20005-3934
(202) 371-2600
1321919_2.DOC

VIII. Claims Appendix (37 C.F.R. § 41.37(c)(1)(viii))

1. A method comprising:

receiving, using a processing device, a first request, from a first sponsor of an access candidate, for access to a first security level in a computer network, wherein the first security level secures computational resources for accessing electronic data;

determining, using the processing device, whether access candidate attributes satisfy access requirements of the resources, wherein the access candidate attributes are revisable based, at least in part, on a determination indicating that access to the first level is prohibited;

granting, using the processing device, access to the first security level based on a determination indicating that access to the first level is not prohibited;

receiving, using the processing device, a second request, from a second sponsor of the access candidate, for access to a second security level in the computer network in response to the granting of access to the first security level, wherein the second security level secures the electronic data;

determining, using the processing device, whether the access candidate attributes satisfy access requirements of the electronic data;

obtaining authorization for the second request from a resolution authority if the access candidate attributes fail to satisfy the access requirements of the electronic data in response to a determination indicating that access to the second security level is prohibited; and

in response to obtaining the authorization from the resolution authority, granting access to the second security level.

2. The method of Claim 1, further comprising granting access to the second security level in response to determining that the access candidate attributes satisfy the access requirements of the electronic data.

3. The method of Claim 1, further comprising denying access to the second security level if the authorization for the second request cannot be obtained.

4. The method of Claim 1, wherein at least one of the access requirements of the resources and the access requirements of the electronic data are represented as part of a graphical display associated with the access candidate and accessed for display to a controller via a network.

5. The method of Claim 1, wherein at least one of the access requirements of the resource and the access requirements of the electronic data comprise a citizenship status of the access candidate or a current location of the access candidate.

6. The method of Claim 5, wherein the access candidate attributes comprise a citizenship status of the access candidate or a current location of the access candidate.

7. A method comprising:

receiving, using a processing device, a first request, from a first sponsor of an access candidate, for physical access to a computer network;

determining, using the processing device, whether access candidate attributes satisfy access requirements of physical access, wherein the access candidate attributes are revisable based, at least in part, on a determination indicating that physical access is prohibited;

granting, using the processing device, the physical access to the computer network based on a determination indicating that physical access is not prohibited;

receiving, using the processing device, a second request, from a second sponsor of the access candidate, for access to electronic data in the computer network in response to the granting of physical access to the computer network;

determining, using the processing device, whether the access candidate attributes satisfy access requirements of the electronic data;

obtaining authorization for the second request from a resolution authority if the access candidate attributes fail to satisfy access requirements of the electronic data in response to a determination indicating that access to the electronic data is prohibited; and

in response to obtaining the authorization from the resolution authority, granting access to the electronic data.

8. The method of Claim 7, further comprising granting access to the electronic data in response to a comparison of the access candidate attributes with the access requirements of the electronic data indicating that access to the electronic data is not prohibited.

9. The method of Claim 7, further comprising denying access to the electronic data if the authorization for the second request cannot be obtained.

10. The method of Claim 7, wherein the access candidate attributes are represented as part of a graphical display associated with the access candidate and accessed for display via a network.

11. The method of Claim 7, wherein at least one of the access requirements of the electronic data and the access requirements of physical access comprise a valid data access agreement with the access candidate; a current location of the access candidate; or a citizenship status of the access candidate.

12. The method of Claim 11, wherein the access candidate attributes comprise an existence of a data access agreement; a current location of the access candidate; or a citizenship status of the access candidate.

13. The method as in Claim 7, wherein at least one of the access requirements of the electronic data and access requirements of physical access comprise a current location of the access candidate or a citizenship status of the access candidate.

14. The method of Claim 7, wherein at least one of the request for physical access or the request for access to the electronic data is submitted by more than one sponsor of the access candidate.

15. A method comprising:

identifying, using a processing device, a plurality of data subsets of electronic data, wherein respective data subsets correspond to respective sets of access requirements;

determining, using the processing device, at least one data class associated with the respective data subsets, the at least one data class identifying at least a citizenship requirement and a location requirement for access to data associated with the at least one data class;

receiving, using the processing device, a first request, from a first sponsor of an access candidate, for access to a first security level in a computer network, wherein the first security level secures physical access to a computer workstation for accessing the electronic data, the first request including access attributes of the access candidate comprising an indication of a citizenship status of the access candidate, an indication of a current location of

the access candidate, and an indication of an existence of a data access agreement with the access candidate;

determining, using the processing device, whether the access candidate attributes satisfy access requirements of the first security level, wherein the access candidate attributes are revisable based, at least in part, on a determination indicating that access to the first security level is prohibited;

granting, using the processing device, access to the first security level based on a determination indicating that access to the first security level is not prohibited;

receiving, using the processing device, a second request, from a second sponsor of the access candidate, for access to a second security level in the computer network in response to the granting of access to the first security level, wherein the second security level secures access to at least one of the plurality of data subsets;

determining, using the processing device, whether the access candidate attributes satisfy the respective set of access requirements corresponding to the at least one of the plurality of data subsets;

obtaining authorization for the second request from a resolution authority if the access candidate attributes fail to satisfy the respective set of access requirements corresponding to the at least one of the plurality of data subsets in response to a determination indicating that access to the at least one of the plurality of data subsets is prohibited; and

in response to obtaining the authorization from the resolution authority, granting access to the second security level.

16. A system comprising:

storage means for receiving and storing electronic data using a computer network;

means for evaluating a first request for access to one or more resources in the computer network, wherein the resources secure the electronic data, wherein an evaluation of the first request includes a first comparison of one or more attributes of the access candidate with one or more access requirements associated with the resources, and wherein the one or more attributes of the access candidate are revisable if the first comparison indicates that access is prohibited;

means for granting access to the one or more resources if the first comparison indicates that access is not prohibited;

means for evaluating a second request for access to the electronic data by the one or more resources, wherein an evaluation of the second request includes a second comparison of the one or more attributes of the access candidate with one or more access requirements associated with the electronic data;

means for obtaining authorization for the second request form a resolution authority if the one or more attributes of the access candidate fails to satisfy one or more access requirements associated with the electronic data in response to the evaluation of the second request indicating that access to the electronic data is prohibited; and

means for granting, in response to obtaining the authorization from the resolution authority, the access candidate access to the electronic data using the one or more resources.

17. The system of Claim 16, further comprising means for granting access to the electronic data using the one or more resources configured to access and manipulate the electronic data if the second comparison indicates that access to the electronic data is not prohibited.

18. The system of Claim 16, wherein the access candidate is denied access to the electronic data if the authorization for the second request cannot be obtained.

19. The system of Claim 16, wherein the one or more access candidate attributes are represented as part of a graphical display associated with the access candidate and accessed for display via a network.

20. The system of Claim 16, wherein at least one of the one or more access requirements associated with the recourses and the one or more access requirements associated with the electronic data relates to at least one of: a valid data access agreement with a potential access candidate; a current location of the potential access candidate; or a citizenship status of the potential access candidate.

21. The system of Claim 20, wherein the one or more access candidate attributes relates to at least one of: an indication an existence of a data access agreement with the access candidate; a current location of the access candidate; or a citizenship status of the access candidate.

22. The system of Claim 16, wherein the one or more access requirements associated with the electronic data includes at least one of a current location of the access candidate or a citizenship status of the access candidate.

23. A system comprising:

storage configured to receive and store electronic data using a computer network;

one or more resources configured to process and manipulate the electronic data using a computer network;

a resource access controller configured to grant access to one or more resources, in response to a request for access to the one or more resources, based at least in part on a comparison of a citizenship status and a current location of an access candidate and an existence of a data access agreement with a citizenship requirement, wherein the location requirement and the data access agreement requirement are associated with the one or more resources;

one or more data access controllers configured to grant access to a corresponding portion of the electronic data based at least in part on a comparison of the citizenship status and the current location of the access candidate with the citizenship requirement and the location requirement associated with the one or more data classes of the corresponding portion of the electronic data;

one or more resolution authorities configured to:

modify access requirements associated with the one or more data classes, and

authorize access to one or more portions of the electronic data in response to a comparison performed by a corresponding data access controller indicating that access is prohibited; and

a data access module configured to:

evaluate a request for access to one or more portions of the electronic data using the one or more resources,

identify one or more data access controllers corresponding to the one or more portions of the electronic data, and

forward the request for access to the one or more identified data access controllers for evaluation regarding whether to grant access to the corresponding one or more portions of the electronic data.

24. A method comprising:

receiving, using a controller in a computer network associated with secured electronic data, a request for access to secured electronic data in the computer network;

comparing, using the controller, one or more attributes of an access candidate with one or more access requirements associated with the secured electronic data;

obtaining authorization for the request from a resolution authority if one or more attributes of the access candidate fails to satisfy one or more access requirements associated with the secured electronic data; and

in response to obtaining or not obtaining authorization from the resolution authority, granting or denying in whole or in part, using the controller, access to the secured electronic data based, at least in part, on a determination based on access candidate information and request related information,

wherein the one or more attributes of the access candidate are revisable based, at least in part, on a determination denying access to the secured electronic data.

25. The method of Claim 24, further comprising granting access to the secured electronic data in response to a comparison indicating that access by the access candidate is not prohibited.

26. The method of Claim 24, wherein the one or more access requirements associated with the secured electronic data are represented as part of a graphical display associated with the access candidate and accessed for display to the controller via a network.

27. The method of Claim 24, wherein the one or more access requirements associated with the secured electronic data are related to at least one of a citizenship status or a current location of the access candidate.

28. The method of Claim 27, wherein the one or more attributes of the access candidate include at least one of a citizenship status or a current location of the access candidate.

29. A method comprising:

receiving, using a controller in a computer network associated with secured electronic data in the computer network, a request for access to the secured electronic data in the computer network;

comparing, using the controller, one or more attributes of an access candidate with one or more access requirements associated with the secured electronic data;

granting, using the controller, access to the secured electronic data in response to a comparison indicating that access by the access candidate is not prohibited;

obtaining authorization for the request from a resolution authority in response to a comparison indicating that access by the access candidate is prohibited; and

in response to obtaining or not obtaining authorization from the resolution authority, granting or denying in whole or in part, using the controller access to the secured electronic data based, at least in part, on a determination based on access candidate information and request related information,

wherein the one or more attributes of the access candidate are revisable based, at least in part, on a determination denying access to the secured electronic data.

30. An article of manufacture including a non-transitory computer-readable medium having instructions stored thereon, execution of which causes a processing device to perform operations comprising:

receiving, using a processing device, a request for access to a first security level in a computer network;

comparing, using the processing device, one or more attributes of an access candidate with one or more access requirements associated with the first security level, wherein the one or more attributes of the access candidate are revisable based, at least in part, on a determination indicating that access by the access candidate to the first security level is prohibited;

granting, using the processing device, access to the first security level based on a comparison indicating that access by the access candidate to the first security level is not prohibited;

receiving, using the processing device, a request for access to a second security level in the computer network;

obtaining authorization for the request from a resolution authority in response to a comparison indicating that access by the access candidate is prohibited.

31. The article of manufacture of Claim 30, further comprising granting access to the second security level in response to a comparison of the one or more attributes of the access candidate with the one or more access requirements associated with the second security level indicating that access to the second security level by the access candidate is not prohibited.

32. The article of manufacture of Claim 30, further comprising denying access to the second security level if the authorization for the request cannot be obtained.

33. The article of manufacture of Claim 30, wherein the one or more attributes of the access candidate is represented as part of a graphical display associated with the access candidate and accessed for display via a network.

34. The article of manufacture of Claim 30, wherein the one or more access requirements associated with the first security level relates to at least one of: a valid data access agreement with the access candidate; a current location of the access candidate; or a citizenship status of the access candidate.

35. The article of manufacture of Claim 34, wherein the one or more attributes of the access candidate relates to at least one of: an indication of whether the access candidate has a data access agreement; a current location of the access candidate; or a citizenship status of the access candidate.

36. The article of manufacture of Claim 30, wherein the one or more access requirements associated with the second security level relates to at least one of a current location of the access candidate or a citizenship status of the access candidate.

37. The article of manufacture of Claim 30, wherein at least one of the request for access to the first security level or the request for access to the second security level is submitted by one or more sponsors.

38. The method as in claim 1, further comprising granting a waiver of the access requirements.

39. (Cancelled)

40. (Cancelled)

41. The method of claim 1, further comprising receiving supplemental evidence verifying the access candidate attributes.

42. The system of claim 15, wherein the data subsets are separated into the at least one data class based on a data provider of the data.

43. The method of claim 15, wherein the physical access comprises physical access to a facility housing the computer workstation.

44. The method of claim 15, wherein the physical access comprises logging on to the computer workstation.

IX. Evidence Appendix (37 C.F.R. § 41.37(c)(1)(ix))

To the best of the knowledge of Appellants, Appellants' legal representative, and Appellants' assignee, there has been no evidence submitted pursuant to 37 C.F.R. §§ 1.130, 1.131, or 1.132, nor has any other evidence been entered in the record by the Examiner and relied upon in this Appeal Brief.

X. Related Proceedings Appendix (37 C.F.R. § 41.37(c)(1)(x))

To the best of the knowledge of Appellants, Appellants' legal representative, and Appellants' assignee, there are no decisions rendered by a court or the board because, as identified above, to the best of the knowledge of Appellants, Appellants' legal representative, and Appellants' assignee, there are no other appeals, interferences, or judicial proceedings which may related to, directly affect, or be directly affected by or have a bearing on a decision by the Board in the pending appeal.